PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-241989
(43)Date of publication of application : 29.08.2003

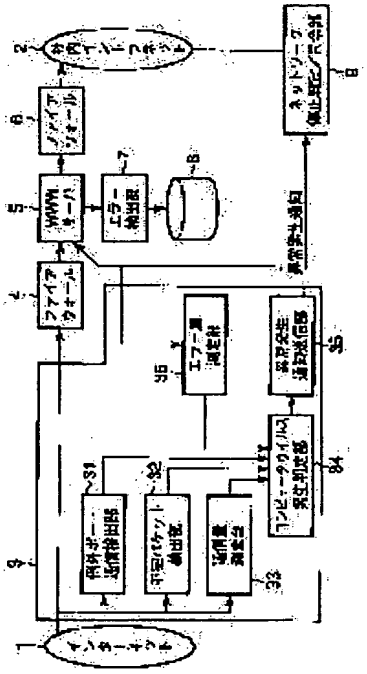
(51)Int.Cl. G06F 11/00
G06F 15/00

(21)Application number : 2002-039087
(22)Date of filing : 15.02.2002

(71)Applicant : TOSHIBA CORP
(72)Inventor : TAKAHASHI TOSHINARI

(54) COMPUTER VIRUS OCCURRENCE DETECTING DEVICE, METHOD AND PROGRAM

(57)Abstract:



PROBLEM TO BE SOLVED: To provide a computer virus occurrence detecting device, method and program capable of early detecting occurrence of computer virus on a network to prevent the infection damage by computer virus on a computer network or computer system that is an object of security protection.
SOLUTION: This computer virus occurrence detecting device 3 early detects whether a computer virus has occurred on Internet 1 or not as the computer virus remains unspecified. Namely, the occurrence of computer virus is detected in a state before the kind or mechanism is clarified and countermeasure data such as vaccine is provided, or an unknown computer virus state. For such a detection, this device is constituted to collect specific data showing the probability of occurrence of computer virus. The specific data is formed of data showing the occurrence of imperfect packet, abnormal increase in communication quantity, abnormal increase in error quantity, or the like, which is caused by a TCP/IP communication using an exceptional port generally not used or an abnormal TCP/IP communication.

LEGAL STATUS

[Date of request for examination]	17.04.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－241989
（Ｐ2003－241989Ａ）
(43)公開日　平成15年８月29日(2003.8.29)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　11/00		Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０７６
15/00	３３０	9/06	６６０Ｎ	５Ｂ０８５

審査請求　有　請求項の数12　ＯＬ　（全９頁）

(21)出願番号　特願2002－39087(Ｐ2002－39087)

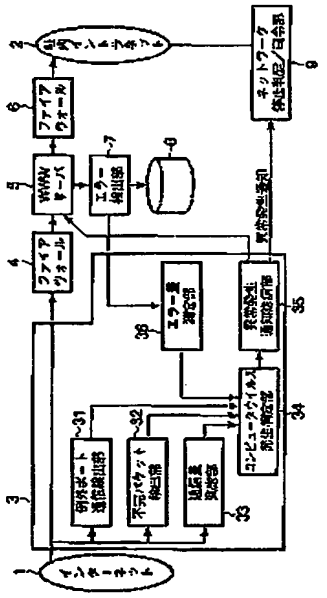
(22)出願日　平成14年２月15日(2002.2.15)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　高橋　俊成
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B076 FD08
5B085 AC14 AE00 BC07

(54)【発明の名称】　コンピュータウイルス発生検出装置，方法，およびプログラム

(57)【要約】
【課題】ネットワーク上でのコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法，およびプログラムを提供すること
【解決手段】コンピュータウイルス発生検出装置３はインターネット１上にコンピュータウイルスが発生したか否かを、同コンピュータウイルスを不特定のまま早期に検出する。すなわち、種別やその仕組み等が明らかとなってワクチン等の対策データが提供される以前の状態、つまり未知コンピュータウイルスの状態でその発生を検出する。かかる検出のために、コンピュータウイルスの発生の可能性を示す特異データを収集するよう構成される。特異データとは、通常は使用されない例外ポートを使用したＴＣＰ／ＩＰ通信が行われたこと、異常なＴＣＰ／ＩＰ通信が行われたことによる不完全なパケットの発生，通信量の異常な増加，エラー量の異常な増加等を示すデータから構成される。



1

【特許請求の範囲】

【請求項１】　コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、

前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、を具備することを特徴とするコンピュータウイルス発生検出装置。

【請求項２】　前記収集手段は、通常は使用しないポートを指定したネットワーク通信の発生有無を、前記特異データとして検出する例外ポート通信検出手段を具備することを特徴とする請求項１に記載のコンピュータウイルス発生検出装置。

【請求項３】　前記収集手段は、所定の通信プロトコルに従うパケット通信処理における通常とは異なる処理の発生を前記特異データとして検出する例外ポート通信検出手段を具備することを特徴とする請求項１に記載のコンピュータウイルス発生検出装置。

【請求項４】　前記収集手段は、前記コンピュータネットワークにおける通信量の異常増加を前記特異データとして検出する通信量測定手段を具備することを特徴とする請求項１に記載のコンピュータウイルス発生検出装置。

【請求項５】　コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置に付帯のコンピュータウイルス発生検出装置であって、

前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、

前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、

前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知手段と、を具備することを特徴とするコンピュータウイルス発生検出装置。

【請求項６】　前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムは、前記通知手段による通知を受けて前記コンピュータウイルスが発生し得るコンピュータネットワークとの接続を遮断する手段を具備することを特徴とする請求項５に記載のコンピュータウイルス発生検出装置。

【請求項７】　前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスを駆除する駆除手段をさらに具備することを特徴とする請求項５又は６に記載のコンピュータウイルス発生検出装置。

【請求項８】　前記収集手段は、ネットワークアクセスにおいて生じたエラー量の異常増加を前記特異データとして測定するエラー量測定手段を具備することを特徴とする請求項５に記載のコンピュータウイルス発生検出装置。

2

【請求項９】　コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法。

【請求項１０】　コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するコンピュータウイルス発生検出方法であって、

前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、

前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法。

【請求項１１】　コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラム。

【請求項１２】　コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するウイルス発生検出プログラムであって、

前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、

前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータシステムのセキュリティに関し、コンピュータネットワーク上におけるコンピュータウイルスの発生を早期に検出するコンピュータウイルス検出装置、方法、およびプログラムに関する。

【０００２】

【従来の技術】近年、コンピュータシステムあるいは個々のハードウエアやソフトウエアを、災害や故障、不正な侵入やコンピュータウイルスなどによる破壊、改変から守るためのセキュリティ技術が注目を集めている。特に、インターネットやイントラネットの急速な普及に応じて、ネットワーク上でのセキュリティが重要視されている。

【０００３】従来、コンピュータウイルスの侵入を防ぐためには、例えばトレンドマイクロ社提供のウイルスバスター等のいわゆるフィルタリングソフトを利用した対策を講じるのが主流である。このフィルタリングソフトでは、ワクチンなどと呼ばれる対策データによりコンピュータウイルスを検出し、これを駆除するようにしている。

【０００４】また、マイクロソフト社のＷｉｎｄｏｗｓ（Ｒ）といったオペレーティングシステム（ＯＳ）のセキュリティホールをついて被害をもたらす類のコンピュータウイルスに対しては、セキュリティホールを埋めるよう手当する修正プログラムを適用し、コンピュータウイルスの被害を防止することも行われている。

【０００５】しかしながら、これら従来のコンピュータウイルス対策はいずれもコンピュータウイルスが発見、特定された後に行われるのであり、新しい（未知の）コンピュータウイルス被害に対して常に後手に回るものである。これは、コンピュータウイルスの発生からその対策までの期間に相当するタイムラグが生じることを意味する。このため、ワクチンや修正プログラムなどの対策データが配布される前の数時間に急速にコンピュータウイルスが蔓延し、多大な被害をもたらすという問題がある。

【０００６】

【発明が解決しようとする課題】いわゆる社内ネットワークなど、ファイアウォールを備えたイントラネット内部へのコンピュータウイルス感染はコンピュータウイルスを含んだ電子メールの受信や、社外ホームページへのアクセスなどといった人間系を起点として発生する。このため、インターネット上でのコンピュータウイルス発生よりも１～１０時間程遅れを生じるのが普通である。また、ほとんどのコンピュータウイルスはｈｔｔｐなどのＴＣＰ／ＩＰ通信を通じて他のコンピュータシステムに順次感染するとされている。

【０００７】本発明はかかる事情を考慮してなされたものであり、ネットワーク上でのコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法、およびプログラムを提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明に係る第１のコンピュータウイルス発生検出装置は、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、を具備することを特徴とするコンピュータウイルス発生検出装置である。

【０００９】本発明に係る第２のコンピュータウイルス発生検出装置は、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置に付帯のコンピュータウイルス発生検出装置であって、前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知手段と、を具備することを特徴とするコンピュータウイルス発生検出装置である。

【００１０】本発明に係る第１のコンピュータウイルス発生検出方法は、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法である。

【００１１】本発明に係る第２のコンピュータウイルス発生検出方法は、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータ

ウイルスの発生を検出するコンピュータウイルス発生検出方法であって．前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと．前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと．を具備することを特徴とするコンピュータウイルス発生検出方法である。

【００１２】本発明に係る第１のコンピュータウイルス発生検出プログラムは、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと．をコンピュータに実行させるコンピュータウイルス発生検出プログラムである。

【００１３】本発明に係る第２のコンピュータウイルス発生検出プログラムは、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するウイルス発生検出プログラムであって．前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと．前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと．をコンピュータに実行させるコンピュータウイルス発生検出プログラムである。

【００１４】

【発明の実施の形態】以下．図面を参照しながら本発明の実施形態を説明する。

【００１５】（第１実施形態）図１は．本発明の第１実施形態に係るコンピュータウイルス発生検出装置の概略構成を示すブロック図である。図１に示すように．インターネット１に対して本発明に係るコンピュータウイルス発生検出装置３が接続されている。また、ＷＷＷサーバ５はファイアウォール４を介してインターネット１に接続されており．社内イントラネット２はファイアウォール６を介してインターネット１に接続されている。ファイアウォール４及び６は．ともに不正なパケットをフィルタリング等するものであり、セキュリティ保護の観点から設けられているが．本発明に必須の構成要素ではない。また図から明らかなようにＷＷＷサーバ５はファイアウォール６を介して社内イントラネット２の外側、すなわちインターネット１側に設けられている。このＷＷＷサーバ５は．同サーバ５に対してなされたアクセスの経過記録（ログ）を保存するアクセスログ保存部８と．このアクセスログ保存部８に保存されているログを参照し、同サーバ５へのアクセスに関して発生したエラーを検出するエラー検出部７を備えている。

【００１６】コンピュータウイルス発生検出装置３は、インターネット１上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する手段として、例外ポート通信検出部３１．不完パケット検出部３２、通信量測定部３３．およびエラー量測定部３６を備えている。また、これら検出部３１，３２及び測定部３３，３６から得られた特異データに基づいて．コンピュータウイルス発生の有無を総合的に判定するコンピュータウイルス発生判定部３４と、該コンピュータウイルス発生判定部３４による判定結果に基づく異常発生通知を外部に報知するための異常発生通知送信部３５を備えている。この異常発生通知送信部３５は、ネットワーク停止判定／司令部９と通信するよう構成されており、ネットワーク停止判定／司令部９は社内イントラネット２に作用し．社内イントラネット２のインターネット１への接続を遮断（ネットワーク停止）したりする。なお．異常発生通知送信部３５を設ける構成とせずに、例えばネットワーク管理者に対して、コンピュータウイルス発生判定部３４により得られた判定結果をディスプレイ等により表示出力するよう構成してもよい。

【００１７】このようなコンピュータウイルス発生検出装置３は、各種コンピュータ上で動作するソフトウェアとして実現可能である。

【００１８】本明細書でいう「コンピュータウイルス」とは．記憶媒体や通信媒体等を通じて伝達し得るプログラム．データ．或いはその組み合わせからなる電子的な情報であって．その情報の受信者が通常想定しない内容または形式のものである。例えば、悪意をもって情報の受信者のコンピュータの動作を異常とする目的の情報が典型的であるが．必ずしも悪意が無くとも不本意に作成されたりまたは不本意な使用法をするなどして想定外のふるまいが起こるもの全てを含む。また、伝達形態や媒体に関して特に制約は無く．記憶媒体に存在したり、ファイルの共有や電子メールによる送信により伝達したり．通常「ワーム」と呼ばれるインターネットを介して増殖する形式のものなど．さまざまな形態が考えられる。また、伝達される個々の情報そのものは通常想定されるものであるが、その組み合わせや伝達の順番．速度等によって同様の効果を生じるものも全体としてコンピュータウイルスと呼ぶことにする。

【００１９】本実施形態のコンピュータウイルス発生検

出装置３は、このようなコンピュータウイルスがインターネット１上に発生したか否かを、同コンピュータウイルスを不特定のまま早期に検出するのであり、すなわち、種別やその仕組み等が明らかとなってワクチン等の対策データが提供される以前の状態、つまり未知コンピュータウイルスの状態でその発生を検出する。かかる検出のために、コンピュータウイルスの発生の可能性を示す特異データを収集するよう構成されている。ここでいう特異データとは、通常は使用されない例外ポートを使用したＴＣＰ／ＩＰ通信が行われたこと、異常なＴＣＰ／ＩＰ通信が行われたことによる不完全なパケットの発生、通信量の異常な増加、エラー量の異常な増加等を示すデータである。

【００２０】図２は本実施形態に係るコンピュータウイルス発生検出装置の概略動作を示すフローチャートである。

【００２１】先ずステップＳ１においてコンピュータウイルス発生検出装置３のインターネット１への接続処理が行われる。インターネット１への接続ののち、エラー量の測定（ステップＳ２）、例外ポート通信の検出（ステップＳ３）、不完パケットの検出（ステップＳ４）、および通信量の測定（ステップＳ５）が行われる。なお、図２においては、ステップＳ２～Ｓ５の処理が並列に実行されるものとして示してあるが、これらを任意の順番で逐次に実行してもよい。

【００２２】これらステップＳ２～Ｓ５の処理においてコンピュータウイルスの発生の可能性を示す特異データが収集され、コンピュータウイルス発生判定部３４に送られる。ステップＳ６において、コンピュータウイルス発生判定部３４は、ステップＳ２～Ｓ５のそれぞれから得られた特異データを元に総合的な判定を行って、未知コンピュータウイルス発生の有無を判定する。ここでの処理は、例えば、測定されたエラー量や通信量を所定のしきい値と比較する処理や、統計学的な処理、ヒューリスティックな処理を含む。

【００２３】次に、ステップＳ７に示すように、コンピュータウイルスが発生したものと判定された場合はステップＳ８に移行する。そうでない場合はステップＳ２～Ｓ５の処理に戻る。

【００２４】ステップＳ８においては、未知コンピュータウイルスが発生した旨の異常発生通知送信部３５がネットワーク停止判定／司令部９に対して送信する。

【００２５】ここで、ステップＳ２におけるエラー量測定に基づくコンピュータウイルス発生判定の流れを図３のフローチャート及び図４乃至図７を参照して説明する。

【００２６】先ずコンピュータウイルス発生検出装置３のエラー量測定部３６は、ＷＷＷサーバ５にアクセスする（ステップＳ１１）。コンピュータウイルスが発生した時点では、未だ社内イントラネット２は同コンピュータウイルスに感染していない。なぜなら、コンピュータウイルスのほとんどは社外イントラネット２の外部（特に海外）から発生し、最初にまず「．ｃｏｍ」ドメインなど在処がはっきりわかっているＷＷＷサーバ５が狙われる。その後に、じわじわと他のサーバにコンピュータウイルスが蔓延し、コンピュータウイルスに感染したＷＷＷサーバ５にユーザがブラウザ等でアクセスすることにより社内イントラネット２が感染するという感染経路となるからである。これをコンピュータウイルス防御の観点から見れば、コンピュータウイルスの発生を最先で発見できるのは最初に狙われるＷＷＷサーバ５であるということができる。

【００２７】エラー量測定部３６は、ＷＷＷサーバ５のエラー検出部７を通じて、アクセスログ保存部８に保存されているアクセスログのうち、エラーが生じたログを要求する。そしてエラー量測定部３６はエラー検出部７から取得したエラーログを解析する（ステップＳ１３）。

【００２８】図４に、通常のアクセスが行われた場合のアクセスログ４０を一例として示す。また、図５は、タイプミスによるエラーが生じた場合のアクセスログ５０を一例として示す。

【００２９】これらは、ユーザがブラウザなどで「http://ホスト/cool/vmware/FAQ.html」というＵＲＬのＷｅｂページにアクセスした場合のログである。図４に示す４１の内容は正しいＵＲＬであるが、図５の５１に示すようにユーザがタイプミスなどすると、当該ＷＷＷサーバ５においては、５０のようなエラーログが記録されることになる。これは、当該ＷＷＷサーバ５においてエラーとして処理されるのであるが、特にコンピュータウイルスを疑う余地はない。

【００３０】一方、図６は異質なアクセスが行われた場合のアクセスログの一例を示す図である。近頃問題となった「Ｎｉｍｄａ」のようなコンピュータウイルスの場合、ＷＷＷサーバ５のセキュリティホールを狙って図６の６０に示すような異質なアクセスがなされ、エラーログとして記録される。

【００３１】これは、図６における６１及び６２からなる非常に長い文字列を含んだＵＲＬを送ることにより、任意のプログラム（文字列６２）をスタックに積んで、これを管理者権限（ｒｏｏｔ権限）で実行させることを目的としており、一般に「アタック（攻撃）」と呼ばれている。アタックは、人間によるコマンド入力操作により行われたり、或いはプログラムにより自動的に行われたりする。

【００３２】図６のような長大なＵＲＬが指定されたアクセスは、ステップＳ１４において異質なアクセスである旨判定される（ステップＳ１４）。これは、ＵＲＬの文字列長を検査することで容易に判定される。

【００３３】図７は異質なアクセスが行われた場合のアクセスログの他の例を示す図である。これは、Ｗｉｎｄｏｗｓ（Ｒ）オペレーティングシステム上で「ｃ：￥ｗｉｎｎｔ￥ｓｙｓｔｅｍ３２￥ｃｍｄ．ｅｘｅ」を起動し、任意のプログラムを実行しようと試みるものである（文字列７１で示される部分）。これもエラーログ７０として記録される。この種のエラーログ７０は、一見して「アタックである」ことが判断できないと考えられるが、明らかにユーザのタイプミスとは区別可能である。

【００３４】コンピュータウイルス発生時には、一時的に、図６或いは図７のようなエラーが急増する。そこでステップＳ１５においては単位時間あたりのエラーの異常増をエラー量測定部３６により測定し、かかる測定結果をコンピュータウイルス発生判定部３４による判定処理に供する。

【００３５】なお、図３においてはステップＳ１４において異質なアクセスである旨判定された場合に速やかにステップＳ１６におけるコンピュータウイルス発生有無の判定に移行しているが、ステップＳ１６に移行する前にエラー量の異常増を判定してもよい。あるいは、図６及び図７に示したような異質なアクセスであるか否かを判定せず、単にエラーの異常増のみを判定することによっても検出能を得ることはできる。

【００３６】コンピュータウイルス発生判定部３４は、エラー量測定部３６により測定されたエラーの異常増を示す特異データを元に、これを所定の閾値と比較するなどしてコンピュータウイルスの発生有無を判定する。なお、この場合の閾値を、ユーザが任意に設定変更できるようユーザインターフェースを設けることが好ましい。

【００３７】コンピュータウイルス発生判定部３４によりコンピュータウイルスが発生した旨の判定が下されると、この情報は異常発生通知送信部３５に送られる。異常発生通知送信部３５は、ネットワーク停止判定／司令部９との通信を確立し、コンピュータウイルス発生の旨を示す異常発生通知を送信する。この異常発生通知を受けたネットワーク停止判定／司令部９は、例えば図８に示すような切断位置でインターネット１との接続を遮断する。

【００３８】このような本実施形態によれば、社内イントラネット２からファイアウォール４、６を介した外側のインターネット１上において、コンピュータウイルスの発生をコンピュータウイルス発生検出装置３によって検出することができ、該コンピュータウイルスの発生を検出した時点で、社内イントラネット２が未感染であることを十分に期待できるようになる。そして、当該コンピュータウイルスに関する詳細情報や対策情報が明らかとなるまでの期間、必要に応じて社内イントラネット２を停止させたり、ＷＷＷなど一部のサービスを停止させることができるようになる。特に、本実施形態によれば

既知のコンピュータウイルスのみならず未知のコンピュータウイルスをもその発生をほぼ完全に検出できるようになる。これは、セキュリティ対策上極めて効果的であり、コンピュータウイルス感染が蔓延して被害が急速に拡大する前に適切な対策を講じることができるようになる。具体的にいうと、コンピュータウイルスは米国時間の昼間に広がることが多いのであるが、日本時間の夜間、つまり従業員の出社前に対策を講じることができるようになる。

【００３９】尚、未知コンピュータウイルスの発生が検出された場合、これが危険なコンピュータウイルスであるか否かについて最終的に人間が判断を下すよう構成することが好ましい。これは、コンピュータウイルス発生判定部３４や異常発生通知送信部３５がシステム管理者等の操作介入を受け付けるよう構成することで実現できる。一方、このような人間による判断を行わず、ネットワーク停止判定／司令部９が自動的にネットワークの停止を行うことは、社内イントラネット２の運用上、支障を来すことも考えられるが、それでも、攻撃にさらされたままにするよりは良いと考えられる。特に、夜間は無条件に社内イントラネット２を停止させることが好ましい。

【００４０】（第２実施形態）上記第１実施形態は、コンピュータウイルス発生検出装置３を、ファイアウォール６を介して社内イントラネット２の外側に設けるものであった。一方、本発明の第２実施形態は、コンピュータウイルス発生検出装置３を社内イントラネット２の内部に設ける構成としたものである。図９はこのような本発明の第２実施形態を示す概略構成図である。

【００４１】コンピュータウイルス発生検出装置３の内部構成は、上記第１実施形態にて説明したものとほぼ同様であるが、本実施形態の場合、アタック検出の対象とするサーバをＷＷＷサーバ５ではなく、図示しない社内イントラネット２内部のサーバとすることができる。このほか、例外ポート通信検出、不完パケット検出、通信量測定についても、社内イントラネット２内を検出又は測定対象とすることができる。このような第２実施形態の場合、社内におけるコンピュータウイルス被害への対策を第１実施形態と同様に早期に行うことができるようになる。また、コンピュータウイルスの発生が社内イントラネット２の外部からのものであることが判明した場合、図９に示すように外部との接続を遮断することもできるようになる。

【００４２】また、本実施形態においては、コンピュータウイルス発生検出装置３と協働する駆除対策部８０が設けられている。この駆除対策部８０は、既知コンピュータウイルスを駆除するための対策データとして、例えばパターンファイルやセキュリティホールを手当する修正プログラム等を社内イントラネット２内のクライアントマシンに配布するものである。なお、このような駆除

11

対策部８０は、上記第１実施形態の構成に付加されてもよいことは勿論である。

【００４３】このような本発明の第２実施形態によっても第１実施形態と同様の作用効果を得ることができる。なお、アタック検出の対象とするサーバを、社内のもののみならず、社外のサーバ（例えばＷＷＷサーバ５）を含め複数台とすれば、コンピュータウイルスの検出性能をさらに高めることができるようになる。

【００４４】なお、本発明は上述した実施形態に限定されず種々変形して実施可能である。例えば、ファイル感染型、マクロ感染等の既知コンピュータウイルスの検出及び対策を本発明の実施と併用することで、セキュリティ対策をより強固なものとすることが好ましい。

【００４５】

【発明の効果】以上説明したように、本発明によれば、ネットワーク上でのコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法、およびプログラムを提供できる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係るコンピュータウイルス発生検出装置の概略構成を示すブロック図。

【図２】上記実施形態に係るコンピュータウイルス発生検出装置の概略動作を示すフローチャート

【図３】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定の流れを示すフローチャート

【図４】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であって、通常のアクセスが行われた場合のアクセスログの一例を示す図

12

＊【図５】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であって、タイプミスによるエラーが生じた場合のアクセスログの一例を示す図

【図６】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であって、異質なアクセスが行われた場合のアクセスログの一例を示す図

【図７】　上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であって、異質なアクセスが行われた場合のアクセスログの一例を示す図

【図８】　上記実施形態に係るコンピュータウイルス発生時における対策処理を説明するための図であって、ネットワークの切断位置を示す図

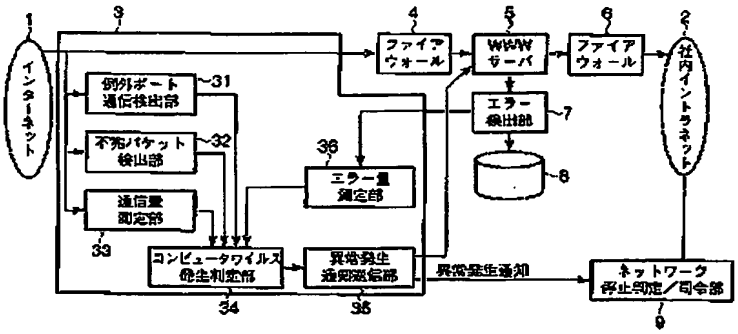
【図９】　本発明の第２実施形態に係る概略構成図

【符号の説明】

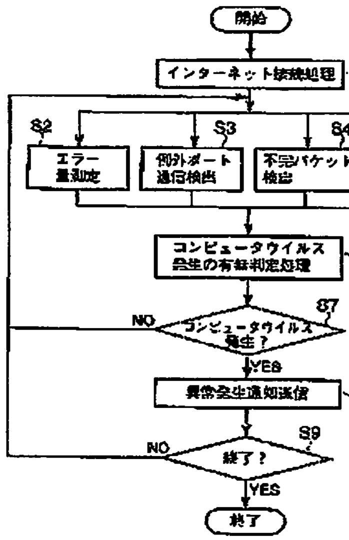
１…インターネット
２…社内イントラネット
３…コンピュータウイルス発生検出装置
４、６…ファイアウォール
５…ＷＷＷサーバ
７…エラー検出部
８…アクセスログ保存部
９…ネットワーク停止判定／司令部
３１…例外ポート通信検出部
３２…不完パケット検出部
３３…通信量測定部
３４…コンピュータウイルス発生判定部
３５…異常発生通知送信部
３６…エラー量測定部

＊

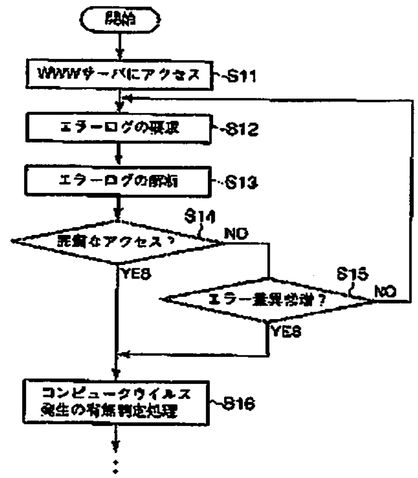
【図１】



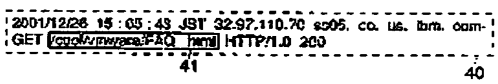
【図2】



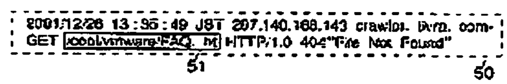
【図3】



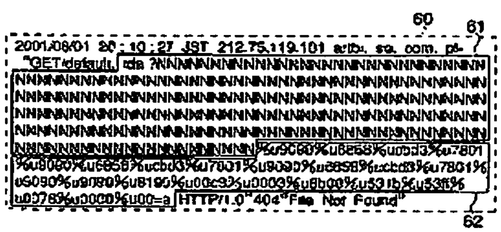
【図4】



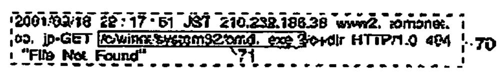
【図5】



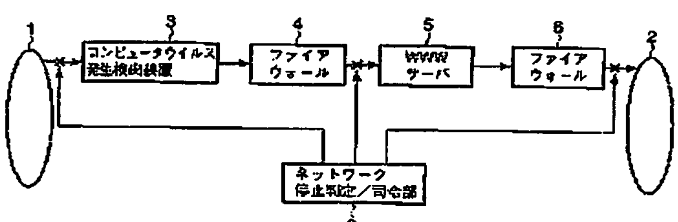
【図6】



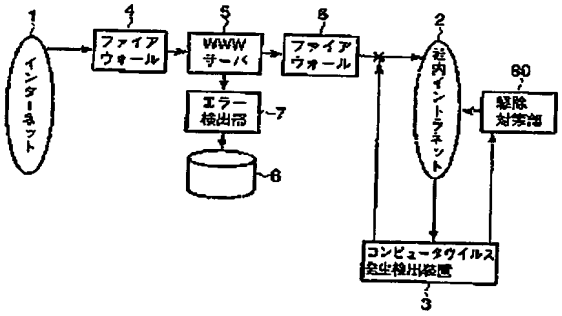
【図7】



【図8】



【図9】


1
インターネット
4
ファイアウォール
5
WWWサーバ
エラー検出部
7
6
8
ファイアウォール
2
社内イントラネット
60
駆除対策部
コンピュータウイルス全生検出装置
3